PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-333407

(43)Date of publication of application : 30.11.2001

(51)Int.Cl. H04N 7/167
H04H 1/00
H04L 9/08
H04L 9/10
H04N 5/44
H04N 5/76
H04N 5/91
H04N 7/08
H04N 7/081
// H04N 7/20

(21)Application number : 2000-153438

(22)Date of filing : 24.05.2000

(71)Applicant : TOSHIBA CORP

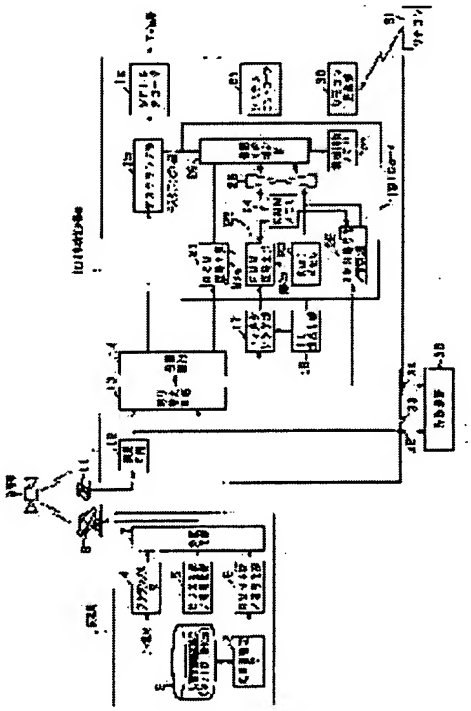
(72)Inventor : OI SHINICHI

(54) PAY BROADCAST SYSTEM, PAY BROADCAST RECEIVER AND PAY BROADCAST TIME SHIFT VIEWING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a pay broadcast system that can prevent illegal viewing in time shift viewing.

SOLUTION: An EMM generating/encryption section 6 of a broadcast station 1 generates an EMM(entitlement management message) that includes information not only at the end of a view contract but also at the start thereof. In the case of time-shift viewing, a view propriety decision section 26 receives the EMM reproduced from a recorder 35. The view propriety decision section 26 uses the information at the start and end of a view contract included in the EMM for the decision of view propriety. Thus, even when the EMM reproduced from the recorder 35 is not compatible with program data and no view contract is made at the broadcast of a reproduced program, the system can prevent illegal viewing.



LEGAL STATUS

[Date of request for examination] 18.02.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－333407
（P2001－333407A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
H04N	7/167		H04H	1/00	F	5C025
H04H	1/00		H04N	5/44	A	5C052
H04L	9/08				Z	5C053
	9/10			5/76	Z	5C063
H04N	5/44			7/20	630	5C064

審査請求　未請求　請求項の数6　ＯＬ　（全 13 頁）　最終頁に続く

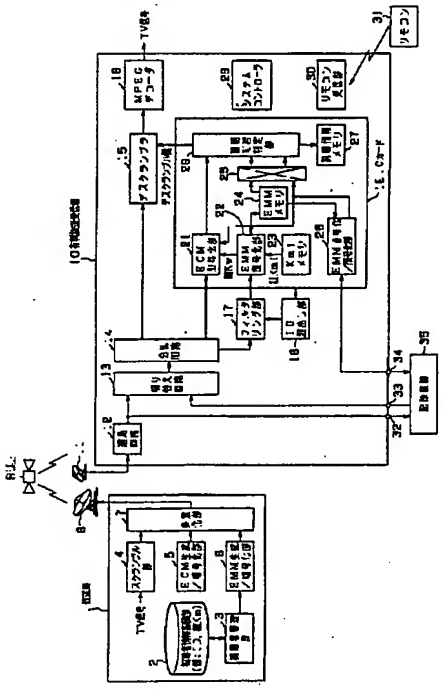
(21)出願番号　特願2000－153438(P2000－153438)
(22)出願日　平成12年５月24日(2000.5.24)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　大井　伸一
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内
(74)代理人　100076233
弁理士　伊藤　進

最終頁に続く

(54)【発明の名称】　有料放送システム、有料放送受信機及び有料放送タイムシフト視聴方法

(57)【要約】
【課題】タイムシフト視聴時における不正視聴を防止する。
【解決手段】放送局１のＥＭＭ生成／暗号化部６は、視聴契約の終了時だけでなく、開始時の情報を含むＥＭＭを生成する。タイムシフト視聴時には記録装置３５から再生されたＥＭＭが視聴可否判定部２６に供給される。視聴可否判定部２６は、視聴可否の判定に際して、ＥＭＭに含まれる視聴契約の開始及び終了時の情報を用いる。これにより、記録装置３５から再生されるＥＭＭと番組データとが対応しない場合であって、再生番組の放送時に視聴契約が行われていない場合であっても、不正視聴を防止することができる。



【特許請求の範囲】
【請求項１】　番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報を暗号化するために用いられるワーク鍵と、視聴契約の内容に応じた情報と、を含む個別情報であって、
前記視聴契約の開始及び終了時の情報を含む個別情報を生成する個別情報生成手段を具備したことを特徴とする有料放送システム。
【請求項２】　番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信手段と、
前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する視聴可否判定手段とを具備したことを特徴とする有料放送受信機。
【請求項３】　番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する受信手段と、
前記受信手段が受信した個別情報を取得する個別情報取得手段と、
前記個別情報取得手段が取得した前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手段と、
前記個別情報取得手段が取得した個別情報と前記番組情報取得手段が取得した番組情報とを組にして暗号化して出力する暗号化手段と、
前記受信手段が受信した番組データ及び前記暗号化手段からの暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手段と、
前記番組情報と前記個別情報とに基いて、番組データの視聴の可否を判定するものであって、
前記記録手段が再生した番組データに含まれる番組情報を前記番組情報取得手段が前記復号化手段からの個別情報中のワーク鍵を用いて復号化して得た番組情報と前記復号化手段からの番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手段とを具備したことを特徴とする有料放送受信機。
【請求項４】　前記個別情報取得手段、前記番組情報取得手段、前記暗号化手段、前記復号化手段及び前記視聴可否判定手段は、集積回路化されていることを特徴とする請求項３に記載の有料放送受信機。
【請求項５】　番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信する手順と、
前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する手順とを具備したことを特徴とする有料放送タイムシフト視聴方法。
【請求項６】　番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する手順と、
受信した個別情報を取得する個別情報取得手順と、
取得された前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手順と、
取得された個別情報と番組情報とを組にして暗号化して出力する暗号化手順と、
番組データ及び前記暗号化手順によって得られた暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手順と、
前記番組情報と前記個別情報とに基いて、番組データの視聴の可否を判定するものであって、
前記記録手段から再生された番組データに含まれる番組情報が前記復号化手順によって得られた個別情報中のワーク鍵を用いて復号化されて番組情報が得られ、得られた番組情報と前記復号化手順によって得られた番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手順とを具備したことを特徴とする有料放送タイムシフト視聴方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、スクランブルされた有料放送番組をそのまま記録し再生時にデスクランブル処理して視聴する有料放送システム、有料放送受信機及び有料放送タイムシフト視聴方法に関する。
【０００２】
【従来の技術】従来、衛星（ＢＳ）を用いた有料のディジタル放送が行われている。有料のＢＳディジタル放送では、放送する番組にスクランブルが施される。視聴者は、放送局と契約することによってスクランブルを解除するスクランブル鍵が与えられる。スクランブル鍵を用いて受信信号をデスクランブルすることにより、番組の視聴が可能となる。

【０００３】放送局では、スクランブル鍵を放送信号に多重して送信する。この場合には、スクランブル鍵は、番組の視聴条件等に関する情報と共にＥＣＭ（EntitlementControl Message）として送信される。

【０００４】一方、視聴者側の受信機は、受信信号をデスクランブルするデスクランブラを有していると共に、デスクランブルに必要なスクランブル鍵を発生するためのカードユニット（ＩＣカード）を備えている。ＩＣカードは、番組の視聴可能な期限等契約条件の情報を含む個別情報（以下、ＥＭＭ（Entitlement Management Message）という）を保持している。なお、ＥＭＭは放送局から送信されて、ＩＣカード内に取込まれることもある。

【０００５】ＩＣカード内においては、受信信号に含まれるＥＣＭからスクランブル鍵を取得し、ＥＣＭと保持しているＥＭＭとから各番組毎に視聴の可否を判定する。ＩＣカードからは、番組視聴可の場合にのみスクランブル鍵がデスクランブラに供給される。これにより、契約条件によって視聴が許可された番組のみが視聴可能となる。

【０００６】ところで、有料放送においても、放送番組をいったん記録し、後に再生して視聴することが考えられる。この場合には、著作権保護の観点から、記録する番組についてはスクランブルをかけたまま記録を行う。ところが、放送局によってＥＭＭが変更されることがある。放送局から変更されたＥＭＭが送信されると、受信機側のＩＣカード内のＥＭＭは更新される。記録されているＥＭＭ変更前の有料放送番組については、変更後のＥＭＭを用いて復号することができないことがある。

【０００７】そこで、番組放送時点におけるＥＭＭを放送番組と共に記録装置に記録することが考えられる。ＩＣカードにＥＭＭの入出力機能を付加すると共に、このようなタイムシフト視聴であるかリアルタイム視聴であるかを判断して、番組の復号に用いるＥＭＭを記録装置から再生したものとＩＣカード内に保持しているものとで切換えるのである。

【０００８】しかしながら、有料放送のこのようなタイムシフト視聴においては、不正視聴が行われることが考えられる。図３乃至図５は不正視聴の例を説明するための説明図である。図３乃至図５は水平方向に時間の経過をとり、また、斜線によって非契約であること及び本来視聴が許可されていない番組であることを示している。

【０００９】図３は放送局と視聴契約していない時点で放送された番組Ａを記録し、契約後に番組Ａを再生する例を示している。図３中の番組Ａは視聴契約していない番組であり、番組Ｂは視聴契約している番組である。また、ＥＭＭは契約前後で変化しないものとし、番組Ｂに対応したＥＭＭで番組Ａも復号可能であるものとする。

【００１０】視聴契約前に番組Ａを記録する時点では、まだ視聴契約が行われていないので、ＥＭＭを番組と同時に記録することはできない。しかし、視聴契約を行えば、番組Ｂの受信時にはＥＭＭを取得することができる。そして、受信機を改造して、再生した番組ＡをリアルタイムＩＣカードに供給することにより、契約後に得られたＩＣカード内のＥＭＭを使用して番組Ａを復号することができる。あるいは、ＩＣカードを制御するコマンドによって、記録装置から再生した番組の復号時であってもＩＣカード内のＥＭＭを使用するように制御することによっても、契約後に得られたＩＣカード内のＥＭＭを使用して番組Ａを復号することができる。

【００１１】図４中の番組Ａは視聴契約していない番組であり、番組Ｂは視聴契約している番組である。また、ＥＭＭは契約前後で変化しないものとする。

【００１２】視聴契約前に番組Ａを記録する。この時点ではＥＭＭを同時に記録することはできない。その後契約を行うことによって、番組Ｂの受信時にＥＭＭを取得することができる。

【００１３】図４に示すように、図３と同様の契約状況において、その後、再び契約を解除するものとする。この場合でも、番組Ｂについては視聴契約があるので、契約時に記録した番組Ｂをタイムシフト視聴することは問題はない。しかし、図３の不正視聴と同様の手法によって、非契約となった後においても、番組Ｂ記録時に記録したＥＭＭを利用することで、番組Ａを復号することが可能となる。

【００１４】図５は特定の番組の視聴契約であるスペシャル契約を一時期行った後、通常のベーシック契約に変更した場合の例である。契約の変更前後においてＥＭＭは変化しないものとする。

【００１５】スペシャル契約時に番組Ｂと共にＥＭＭを記録装置に記録する。その後契約をベーシック契約に変更し、ベーシック契約となった以降の番組Ｃを記録する。この場合でも、番組ＢのＥＭＭによって番組Ｃの復号が可能であるものとすると、図３の不正視聴と同様の手法によって、スペシャル契約時に記録したＥＭＭを利用して、ベーシック契約後に記録した番組Ｃの復号が可能である。

【００１６】

【発明が解決しようとする課題】このように、従来、タイムシフト視聴では、視聴契約した番組に対応していないＥＭＭを利用して不正視聴されてしまうことがあるという問題点があった。

【００１７】本発明はかかる問題点に鑑みてなされたものであって、タイムシフト視聴を可能にした場合でも、不正視聴を確実に防止することができる有料放送システム、有料放送受信機及び有料放送タイムシフト視聴方法を提供することを目的とする。

【００１８】

【課題を解決するための手段】本発明の請求項１に係る

有料放送システムは、番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報を暗号化するために用いられるワーク鍵と、視聴契約の内容に応じた情報と、を含む個別情報であって、前記視聴契約の開始及び終了時の情報を含む個別情報を生成する個別情報生成手段を具備したものであり、本発明の請求項２に係る有料放送受信機は、番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信手段と、前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する視聴可否判定手段とを具備したものであり、本発明の請求項３に係る有料放送受信機は、番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する受信手段と、前記受信手段が受信した個別情報を取得する個別情報取得手段と、前記個別情報取得手段が取得した前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手段と、前記個別情報取得手段が取得した個別情報と前記番組情報取得手段が取得した番組情報とを組にして暗号化して出力する暗号化手段と、前記受信手段が受信した番組データ及び前記暗号化手段からの暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手段と、前記番組情報と前記個別情報とに基いて、番組データの視聴の可否を判定するものであって、前記記録手段が再生した番組データに含まれる番組情報を前記番組情報取得手段が前記復号化手段からの個別情報中のワーク鍵を用いて復号化して得た番組情報と前記復号化手段からの番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手段とを具備したものであり、本発明の請求項５に係る有料放送タイムシフト視聴方法は、番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報であって前記視聴契約の開始及び終了時の情報を含む個別情報と、を受信する受信する手順と、前記視聴契約の開始及び終了時の情報を用いて、番組データの視聴の可否を判定する手順とを具備したものであり、本発明の請求項６に係る有料放送タイムシフト視聴方法は、番組データと、前記番組データのスクランブルに用いたスクランブル鍵及び番組を特定するための情報を有する番組情報と、前記番組情報を暗号化するために用いられるワーク鍵及び視聴契約の内容に応じた情報を有する個別情報と、を受信する手順と、受信した個別情報を取得する個別情報取得手順と、取得された前記個別情報中のワーク鍵を用いて前記番組情報を復号化する番組情報取得手順と、取得された個別情報と番組情報とを組にして暗号化して出力する暗号化手順と、番組データ及び前記暗号化手順によって得られた暗号出力が記録された記録手段から前記番組データを再生してタイムシフト視聴する場合に、前記暗号出力を復号化して前記個別情報及び前記番組情報の組を取得する復号化手順と、前記番組情報と前記個別情報とに基いて、番組データの視聴の可否を判定するものであって、前記記録手段から再生された番組データに含まれる番組情報が前記復号化手順によって得られた個別情報中のワーク鍵を用いて復号化されて番組情報が得られ、得られた番組情報と前記復号化手順によって得られた番組情報との同一性の判定を行い、同一であると判定した場合にのみ前記視聴の可否の判定結果を有効とし、同一でないと判定した場合には視聴不可と判定する視聴可否判定手順とを具備したものである。

【００１９】本発明の請求項１において、個別情報生成手段は、視聴契約の開始及び終了時の情報を含む個別情報を生成する。これにより、受信側で、視聴契約の終了時だけでなく開始時の情報を利用した視聴可否の判定を可能にする。

【００２０】本発明の請求項２において、受信手段は、番組データ、番組情報及び個別情報を受信する。個別情報には、視聴契約の開始及び終了時の情報が含まれる。視聴可否判定手段は、視聴契約の終了時の情報だけでなく、開始時の情報を用いて、番組データの視聴の可否を判定する。

【００２１】本発明の請求項３において、受信手段は、番組データ、番組情報及び個別情報を受信する。個別情報取得手段が取得した個別情報と番組情報取得手段が取得した番組情報とは、暗号化手段によって、組にされて暗号化される。記録された番組データをタイムシフト視聴する場合には、組にされて暗号化された個別情報及び番組情報は、復号化手段によって復号される。再生された番組データに含まれる番組情報は、番組情報取得手段によって、復号化手段からの個別情報を用いて復号化される。判定手段は、番組情報取得手段からの番組情報と復号化手段からの番組情報との同一性を判定する。判定手段は、同一でない場合には、視聴不可と判定し、同一であると判定した場合にのみ、番組情報と個別情報とに基く視聴可否の判定を有効とする。

【００２２】本発明の請求項５において、前記視聴契約の開始及び終了時の情報を含む個別情報を受信する。この視聴契約の開始及び終了時の情報を用いて、番組デー

タの視聴の可否を判定する。

【００２３】本発明の請求項６において、番組データと、番組情報と、個別情報とを受信する。受信した個別情報を取得し、取得された個別情報中のワーク鍵を用いて番組情報を復号化する。暗号化手順では、取得された個別情報と番組情報とを組にして暗号化して出力する。記録手段に記録された番組データを再生してタイムシフト視聴する場合には、復号化手順は、暗号化された個別情報と番組情報との組を復号化して個別情報及び前記番組情報の組を取得する。復号された個別情報を用いて、再生された番組データに含まれる番組情報を復号化する。番組情報と復号化手順による番組情報とについては、視聴可否判定手順において同一性を判定する。同一でない場合には、視聴不可と判定し、同一であると判定した場合にのみ、番組情報と個別情報とに基く視聴可否の判定が有効となる。

【００２４】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。図１は本発明の一実施の形態に係る有料放送システム及び有料放送受信機を示すブロック図である。

【００２５】放送局１は有料放送の放送信号を送信する。番組を構成する映像信号及び音声信号等は例えばＭＰＥＧ規格で符号化され、番組のトランスポートストリーム（Transport Stream）がＴＶ（テレビジョン）信号としてスクランブル部４に供給される。放送局１は、有料の放送番組にはスクランブルを施す。スクランブル部４は、入力されたＴＶ信号に対して所定のスクランブル鍵を用いたスクランブル処理を施して多重化部７に与える。

【００２６】有料放送においては、視聴者は、放送局と視聴契約を結ぶことによって、有料放送番組を受信して視聴することができる。受信側では、契約条件等に応じて、視聴可と判定された番組については、スクランブル鍵を用いてデスクランブル処理することによって、有料放送番組の視聴を行う。このような視聴可否の判定をＩＣカードを用いて行うことがある。

【００２７】例えば、日本のＣＳを利用した放送であるスカイパーフェクＴＶやディレクＴＶ等の放送を受信する機器においては、視聴可否の判定にＩＣカードが利用されている。ＩＣカードは、カードを識別するためのカードＩＤ及びカード毎に固有のマスター鍵Ｋｍ を記憶している。ＩＣカードは、後述するように、マイコン装置であり、マイコン内の不揮発メモリに契約条件等の情報を記憶し、番組受信時に番組の情報と契約条件等の情報とに基いて視聴可否を判定するのである。

【００２８】このような視聴可否の判定のために、ＥＣＭ及びＥＭＭが用いられる。ＥＣＭは、社団法人電波産業会が策定したＢＳデジタル放送限定受信方式の標準規格のＡＲＩＢ　ＳＴＤ－Ｂ２５　１．０版（以下、標準規格という）にて規定されている。この規定によれば、ＥＣＭは、常に固定的に伝送される固定部と、目的によって内容が異なる可変部とによって構成される。ＥＣＭ固定部には、プロトコル番号、有料事業体識別、ワーク鍵識別、番組に施したスクランブルのスクランブル鍵、判定タイプ、年月日時分、録画制御及び改ざん制御が配置される。また、ＥＣＭ可変部には、ティア（定額）判定に関する機能情報、従量課金（ＰＰＶ（ペイパービュー））判定に関する機能情報及び消去に関する機能情報が配置される。即ち、ＥＣＭによって、番組を特定する情報及び録画の可否等を示す情報が伝送される。

【００２９】また、ＥＭＭについても、標準規格にて規定されている。この規定によれば、ＥＭＭは、常に固定的に伝送される固定部と、目的によって内容が異なる可変部とによって構成される。ＥＭＭ可変部には、各種機能情報、即ち、ワーク鍵に関する機能情報、ティアに関する機能情報、後払いＰＰＶに関する機能情報、通電制御に関する機能情報、全体制御に関する機能情報及び強制発呼に関する機能情報が配置される。また、ＥＭＭ固定部には、カードＩＤ、関連情報バイト長、プロトコル番号、有料事業体識別、更新番号及び契約の終了時を示す有効期限の情報が配置される。ＥＭＭのうちカードＩＤを除く部分については後述するように暗号化されるようになっている。

【００３０】ＥＣＭ生成／暗号化部５は、番組毎にＥＣＭを生成する。上述したように、ＥＣＭにはスクランブル鍵が含まれており、ＥＣＭ生成／暗号化部５は、ワーク鍵Ｋｗ を用いて、生成したＥＣＭを暗号化した後、多重化部７に出力するようになっている。受信側では、ワーク鍵Ｋｗ を用いることで、ＥＣＭを復号化してスクランブル鍵を得ることができる。

【００３１】放送局１は、視聴契約が変更されること及び不正視聴を防止するために、ワーク鍵Ｋｗ を適宜変更するようになっている。このため、放送局１は、ワーク鍵Ｋｗ についても、多重化して送信するようになっている。上述したように、ＥＭＭ可変部にワーク鍵Ｋｗ に関する情報を配置する。

【００３２】ＥＭＭ生成／暗号化部６は、ＥＭＭを生成するようになっている。ＥＭＭ生成／暗号化部６は、視聴契約に応じて、ＥＭＭを個別の宛先に送信する。即ち、ＥＭＭ生成／暗号化部６は、ＥＭＭ固定部に、非暗号のカードＩＤを配置することで、受信側が自己宛のＥＭＭを識別することを可能にする。カードＩＤは視聴契約に際して放送局１に与えられる。

【００３３】即ち、視聴者が放送局１との間で視聴契約を結ぶ場合には、視聴者は受信機に取り付けるＩＣカードの情報を放送局１に与えるようになっている。放送局１は、視聴者情報蓄積部２において、ユーザーとＩＤ、ＩＤとマスター鍵Ｋｍ との関係を記述した視聴者情報を保持している。視聴者管理部３は、視聴契約に応じて視

聴情報蓄積部２に保持する視聴者情報を更新すると共に、各ユーザー毎のＩＤ及びマスター鍵Ｋｍを読出してＥＭＭ生成／暗号化部６に出力するようになっている。

【００３４】本実施の形態においては、ＥＭＭ生成／暗号化部６は、ＥＭＭ固定部に配置する有効期限に関する情報に、契約の開始を示す情報を加えるようになっている。ＥＭＭ生成／暗号化部６は、契約の開始及び終了時を示す情報を含むＥＭＭ固定部とワーク鍵Ｋｗや契約条件を含むＥＭＭ可変部とを生成し、カードＩＤを除く部分についてはマスター鍵Ｋｍを用いて暗号化する。ＥＭＭ生成／暗号化部６からのＥＭＭは多重化部７に供給される。

【００３５】多重化部７は、スクランブル部５の出力、ＥＣＭ生成／暗号化部５の出力及びＥＭＭ生成／暗号化部６の出力を多重化して、アンテナ８から送信するようになっている。アンテナ８からの放送信号は衛星９によって放送される。

【００３６】一方、有料放送受信機１０においては、衛星９からの放送信号をアンテナ１１によって受信する。アンテナ１１からの高周波信号は選局回路１２に供給され、選局回路１２は、システムコントローラ２９から指示されたチャンネルの番組を選択して、番組データを出力する。選局回路１２の出力は、切り替え回路１３に供給されると共に、端子３２を介して記憶装置３５にも供給される。

【００３７】なお、システムコントローラ２９はユーザ操作に基いて選局チャンネルを切換える。ユーザは例えばリモコン３１によって有料放送受信機１０を制御する。リモコン３１は、ユーザ操作に基く信号を送信し、リモコン受信部３０は、リモコン３１からの信号を受信してシステムコントローラ２９に与える。これにより、システムコントローラ２９は、ユーザ操作に基いて、有料放送受信機１０の各部を制御するようになっている。

【００３８】記録装置３５は、端子３２を介して選局回路１２からの番組データが与えられ、ユーザ操作に応じて入力された番組データを所定の記録媒体に記録する。また、記録装置３５は、記録媒体に記録されている番組データを再生して、端子３３を介して有料放送受信機１０に出力することができるようになっている。

【００３９】更に、記録装置３５は、端子３４を介して有料放送受信機１０に接続されており、有料放送受信機１０に挿着されたＩＣカード１９内のＥＭＭ暗号化／復号化部２８からのＥＭＭ信号を、選局回路１２からの番組データに対応させて記録媒体に記録すると共に、記録されたＥＭＭ信号を再生してＥＭＭ暗号化／復号化部２８に出力することができるようになっている。

【００４０】なお、記録装置３５としては種々の装置を利用可能である。例えば、ＤＶＤ、ハードディスク等を利用した機器、ディジタルＶＴＲ等種々考えられる。また、受信機１０と記録装置３５との間の接続についても規定しない。

【００４１】また、スクランブルされた番組を入出力する端子３２，３３とＥＭＭを入出力する端子３４とを別々のものとしたが、番組にＥＭＭを多重した形で入出力する場合も考えられる。

【００４２】切り替え回路１３は、放送番組を視聴する場合には、選局回路１２の出力を選択して分離回路１４に与え、記録している番組を視聴する場合には、端子３３からの記録装置３５の出力を選択して分離回路１４に与えるようになっている。分離回路１４は、入力された番組データ中に含まれる番組のストリーム、ＥＣＭ及びＥＭＭを分離し、夫々、デスクランブラ１５、ＩＣカード１９及びフィルタリング部１７に出力する。

【００４３】デスクランブラ１５は、後述するように、ＩＣカード１９からデスクランブル鍵が与えられて、入力されたストリームをデスクランブル処理してＭＰＥＧデコーダ１６に出力する。ＭＰＥＧデコーダ１６は、入力されたトランスポートストリームをデコードして、番組の映像信号及び音声信号等（ＴＶ信号）を図示しないモニタに出力するようになっている。

【００４４】ＩＣカード１９は、カードＩＤを図示しない記憶部に記憶している。ＩＤ読出し部１８は、ＩＣカード１９からカードＩＤを読出して、フィルタリング部１７に供給するようになっている。フィルタリング部１７は、分離回路１４から与えられたＥＭＭに含まれるカードＩＤとＩＤ読出し部１８からのカードＩＤとを比較することによって、自機宛のＥＭＭを識別する。フィルタリング部１７は、自機宛のＥＭＭは、ＩＣカード１９に出力するようになっている。

【００４５】分離回路１４からのＥＣＭは、ＩＣカード１９のＥＣＭ復号化部２１に与えられ、フィルタリング部１７からのＥＭＭはＥＭＭ復号化部２２に与えられる。ＩＣカード１９は、マスター鍵Ｋｍを格納しているＫｍｉメモリ２３を有している。ＥＭＭ復号化部２２はＫｍｉメモリ２３からのマスター鍵Ｋｍを用いてＥＭＭを復号化する。これにより、ＥＭＭに含まれるワーク鍵Ｋｗ及びその他の情報が得られる。ＥＭＭ復号化部２２は、復号したＥＭＭ（ワーク鍵Ｋｗを含む）をＥＭＭメモリ２４に出力すると共に、ワーク鍵ＫｗをＥＣＭ復号化部２１に出力する。

【００４６】ＥＣＭ復号化部２１は、ＥＭＭ復号化部２２又は後述するＥＭＭ暗号化／復号化部２８からのワーク鍵Ｋｗを用いて、分離回路１４からのＥＣＭを復号化する。これにより、ＥＣＭに含まれるスクランブル鍵及びその他の情報が得られる。ＥＣＭ復号化部２１の復号出力は視聴可否判定部２６に与えられる。

【００４７】ＥＭＭメモリ２４は入力されたＥＭＭを保持し、放送局１によってＥＭＭが更新されるまで、保持しているＥＭＭをＥＭＭ復号化部２２に与えると共に、セレクタ２５を介して視聴可否判定部２６に与える。ま

た、ＥＭＭメモリ２４は保持しているＥＭＭをＥＭＭ暗号化／復号化部２８にも出力するようになっている。ＥＭＭ暗号化／復号化部２８はＥＭＭメモリ２４からのＥＭＭを暗号化して、端子３４から記憶装置３５に供給するようになっている。また、ＥＭＭ暗号化／復号化部２８は、記憶装置３５から再生されたＥＭＭが端子３４を介して入力され、入力されたＥＭＭを復号化して復号出力をセレクタ２５に出力すると共に、復号出力に含まれるワーク鍵Ｋｗ をＥＣＭ復号化部２１に出力するようになっている。

【００４８】セレクタ２５は、リアルタイム視聴時にはＥＭＭメモリ２４からのＥＭＭを選択し、タイムシフト視聴時にはＥＭＭ暗号化／復号化部２８からのＥＭＭを選択して視聴可否判定部２６に出力する。

【００４９】視聴可否判定部２６は、入力されたＥＣＭとＥＭＭとを対比し、デスクランブラに入力された番組データが視聴許可されているか否かを判定する。視聴可否判定部２６は、視聴可であると判定した場合には、ＥＣＭ復号化部２１からのスクランブル鍵をデスクランブル鍵としてデスクランブラ１５に与える。視聴可否判定部２６は、視聴不可と判定した場合には、スクランブル鍵を出力しない。従って、この場合には、デスクランブラ１５はデスクランブル処理を行うことができず、番組を正常に視聴することはできない。

【００５０】本実施の形態においては、視聴可否判定部２６は、視聴可否の判定に際して、視聴契約の期限の情報、即ち、視聴契約の終了時の情報だけでなく、視聴契約の開始時の情報も用いるようになっている。即ち、視聴可否判定部２６は、入力されたＥＭＭ中の視聴契約開始時の情報によって示される視聴契約開始時がＥＣＭによって示される番組の放送日時よりも前でない場合には、視聴不可と判定するようになっている。つまり、視聴可否判定部２６は、入力されたＥＭＭ中の視聴契約開始及び終了時の情報によって示される視聴契約開始から終了までの間に、ＥＣＭによって示される番組の放送が行われている場合にのみ視聴可と判定する。

【００５１】視聴可否判定部２６は、視聴可と判定した場合には、視聴情報メモリ２７に視聴情報を出力するようになっている。ＰＰＶ（ペイパービュー）では、番組毎に購入，非購入を決定することができる。視聴情報メモリ２７は、購入した（視聴した）ＰＰＶの番組を特定するための情報を視聴情報として記憶するようになっている。なお、視聴情報メモリ２７に格納された視聴情報は、図示しない電話回線等によって、放送局に伝送され、視聴料の精算に用いられる。

【００５２】次に、このように構成された実施の形態の動作について説明する。

【００５３】放送局１は、スクランブル部４によって番組ストリームにスクランブルをかける。ＥＣＭ生成／暗号化部５はスクランブル鍵を含むＥＣＭを生成して、ワーク鍵Ｋｗ によって暗号化する。視聴者情報蓄積部２は、各ユーザ、カードＩＤ及びマスター鍵Ｋｍ の情報を含む視聴者情報を蓄積している。ＥＭＭ生成／暗号化部６は、所定のタイミングで、ワーク鍵Ｋｗ 及びカードＩＤを含むＥＭＭを作成し、カードＩＤを除く部分をマスター鍵Ｋｍ を用いて暗号化する。

【００５４】本実施の形態においては、ＥＭＭ生成／暗号化部６は、ＥＭＭ固定部には、視聴契約の開始及び終了時を示す期限情報を配置する。スクランブルが施された番組ストリーム及び暗号化されたＥＣＭ，ＥＭＭは、多重化部７において多重化され、アンテナ８から送信される。

【００５５】一方、受信側においては、アンテナ１１を介して受信した放送信号は、選局回路１２によって所定チャンネルの番組が選局される。いま、リアルタイム視聴を行うものとする。この場合には、切り替え回路１３は選局回路１２の出力を選択して分離回路１４に出力する。分離回路１４によって、切り替え回路１３の出力に含まれる番組データ、ＥＣＭ，ＥＭＭは、夫々デスクランブラ１５、ＥＣＭ復号化部２１及びフィルタリング部１７に供給される。

【００５６】ＩＤ読出し部１８は、ＩＣカード１９からカードＩＤを読出してフィルタリング部１７に供給する。フィルタリング部１７は、カードＩＤを比較することによって、分離回路１４の出力から自機宛のＥＭＭをフィルタリングしてＩＣカード１９に出力する。

【００５７】ＩＣカード１９のＥＭＭ復号化部２２は、Ｋｍｉメモリ２３からマスター鍵Ｋｍ を読出して、ＩＣカード１９に入力されたＥＭＭを復号し、ＥＭＭメモリ２４に出力する。また、ＥＭＭ復号化部２２はＥＭＭに含まれるワーク鍵Ｋｗ をＥＣＭ復号化部２１に与える。このワーク鍵Ｋｗ を用いて、ＥＣＭ復号化部２１は、分離回路１４からのＥＣＭを復号する。これにより、ＥＣＭ復号化部２１はスクランブル鍵を含むＥＣＭを得て視聴可否判定部２６に出力する。

【００５８】なお、放送局１からの放送信号に自機宛のＥＭＭが含まれない場合には、ＥＭＭ復号化部２２はＥＭＭメモリ２４に格納されているＥＭＭ中のワーク鍵Ｋｗ をＥＣＭ復号化部２１に出力する。

【００５９】セレクタ２５はＥＭＭメモリ２４からのＥＭＭを視聴可否判定部２６に出力する。視聴可否判定部２６は、ＥＣＭとＥＭＭとに基いて、デスクランブラ１５に入力されている番組データが視聴可の番組のものであるか否かを判定する。ユーザがリモコン３１で視聴を希望したチャンネル（番組）は、視聴契約によって視聴が許可されているものであるものとすると、視聴可否判定部２６は、スクランブラ１５に入力されている番組データが視聴可の番組のものであるものと判定し、ＥＣＭに含まれるスクランブル鍵をデスクランブル鍵としてデスクランブラ１５に出力する。

【００６０】デスクランブラ１５は、デスクランブル鍵を用いて番組データのスクランブルを解除する。デスクランブラ１５からの番組ストリームはＭＰＥＧデコーダ１６に供給され、デコードされてＴＶ信号が得られる。このＴＶ信号をモニタに供給することによって、ユーザが指定した番組の視聴が可能となる。

【００６１】また、ユーザが指定した番組が視聴契約されていない場合には、視聴可否判定部２６は、ＥＣＭ，ＥＭＭから視聴不可であるものと判定し、スクランブル鍵を出力しない。従って、この場合には、ユーザが指定した番組のデスクランブル処理は行われず、番組を正常に視聴することはできない。

【００６２】なお、視聴可否判定部２６は、視聴可否の判定を行った番組がＰＰＶである場合には、視聴情報を視聴情報メモリ２７に格納する。

【００６３】次に、ユーザが番組の記録を指示するものとする。この場合には、選局回路１２からの番組データは、端子３２を介して記録装置３５に供給され、記録媒体上に記録される。

【００６４】また、切り替え回路１３は選局回路１２の出力を分離回路１４に与える。こうして、番組の記録時においても、ＥＭＭがフィルタリング部１７からＩＣカード１９に供給される。ＥＭＭ復号化部２３は、Ｋｍｉメモリ２３から読出したマスター鍵Ｋｍ を用いてＥＭＭを復号し、復調出力をＥＭＭメモリ２４に出力する。ＥＭＭメモリ２４はＥＭＭ復号化部２２の出力によって記録しているＥＭＭを更新する。なお、自機宛のＥＭＭが放送されない場合には、ＥＭＭメモリ２４は保持しているＥＭＭを更新しない。

【００６５】番組の記録時には、ＥＭＭメモリ２４は保持しているＥＭＭをＥＭＭ暗号化／復号化部２８に出力する。ＥＭＭ暗号化／復号化部２８は、入力されたＥＭＭを暗号化してＩＣカード１９から出力する。暗号化されたＥＭＭは端子３４から記録装置３５に供給され、記録装置３５は暗号化されたＥＭＭを対応する番組データと共に記録媒体に記録する。

【００６６】次に、ユーザが記録装置３５に記録されている番組を再生して視聴するものとする。この場合には、システムコントローラ２９は、切り替え回路１３に記録装置３５の出力を選択させると共に、セレクタ２５にＥＭＭ暗号化／復号化部２８の出力を選択させる。記録装置３５からの番組データは切り替え回路１３を介して分離回路１４に供給される。また、記録装置３５から再生された番組データに対応するＥＭＭは、端子３４からＩＣカード１９内のＥＭＭ暗号化／復号化部２８に供給される。ＥＭＭ暗号化／復号化部２８は再生されたＥＭＭを復号して出力する。

【００６７】分離回路１４は、再生出力中の番組データをデスクランブラ１５に出力し、ＥＣＭをＥＣＭ復号化部２１に出力する。ＥＣＭ復号化部２１は、ＥＭＭ暗号化／復号化部２８からのＥＭＭに含まれるワーク鍵Ｋｗを用いて、ＥＣＭを復号化する。ＥＣＭ復号化部２１は復号したＥＣＭを視聴可否判定部２６に出力する。セレクタ２５はＥＭＭ暗号化／復号化部２８からのＥＭＭを視聴可否判定部２６に出力する。

【００６８】このように、視聴可否判定部２６には、番組放送当時の番組に対応したＥＣＭとこの番組に対応したＥＭＭとが入力される。視聴可否判定部２６は入力されたＥＣＭ，ＥＭＭから視聴可否を判定する。番組放送当時に、記録した番組についての視聴契約が結ばれている場合には、視聴可否判定部２６は入力されたＥＣＭ，ＥＭＭから視聴可と判定することができる。逆に、記録した番組についての視聴契約が結ばれていない場合には、視聴可否判定部２６は入力されたＥＣＭ，ＥＭＭから視聴不可と判定することができる。こうして、記録装置３５に記録された番組をタイムシフト視聴する場合においても、視聴契約に応じた視聴が行われる。

【００６９】また、視聴契約を途中で変更した場合、例えば、ある月の月末に記録した番組を、翌日（翌月）に視聴する場合において、その月変わりで契約を変更し、翌月から記録した番組を放送するチャンネルの契約が無くなる場合等であっても、記録した番組とこの番組に対応するＥＭＭを視聴可否の判定に用いることができるので、正常にタイムシフト視聴が可能である。

【００７０】ここで、ユーザの不正によって、記録装置３５から再生された番組と対応しないＥＭＭが視聴可否判定部２６に入力されるものとする。例えば、番組Ａ，Ｂ等に対する視聴契約が図３又は図４に示す状況であるものとし、視聴契約が結ばれていない番組Ａの再生時に、視聴契約された番組Ｂに対応するＥＭＭが視聴可否判定部２６に入力されるものとする。なお、番組Ｂに対応するＥＭＭは、従来と同様の視聴可否の判定方法によれば、番組Ａの復号を可能にするものとする。即ち、番組Ｂに対応するＥＭＭは、ワーク鍵Ｋｗ が番組Ａに用いられたものと同一であり、また、視聴契約の終了時は番組Ａの放送日時よりも後に設定されている。

【００７１】しかし、視聴可否判定部２６は、ＥＭＭに含まれる視聴契約の開始時の情報も用いて視聴可否を判定する。即ち、図３及び図４の場合には、番組Ｂに対応するＥＭＭ中には、視聴契約の開始時が番組Ａの放送日時よりも後の日時を示す情報が記述されていることから、視聴可否判定部２６は、番組Ａに対応するＥＣＭと番組Ｂに対応するＥＭＭとが入力された場合でも、番組Ａについては視聴不可と判定する。

【００７２】これにより、視聴契約を行っていない番組Ａについては、対応していないＥＭＭを用いた不正視聴をユーザが試みても、正常にタイムシフト視聴することはできない。

【００７３】このように、本実施の形態においては、ＥＭＭ内の視聴契約の期限情報として、視聴契約の終了時

だけでなく開始時の情報も含めて送信し、ＥＣＭ内の時刻情報と比較してＥＭＭの視聴契約の始まりを示す情報が時間的に前であり、かつ契約の終わりを示す時刻情報が時間的に後であることを条件に視聴可とするようにしているので、ユーザが再生する番組に対応していないＥＭＭを不正に利用してタイムシフト視聴しようとしても、視聴を不許可にすることができ、不正視聴を防止することができる。

【００７４】図２は本発明の他の実施の形態を示すブロック図である。図２において図１と同一の構成要素には同一符号を付して説明を省略する。図１の実施の形態においては、図５の場合については不正視聴を阻止することはできない。本実施の形態においては図３乃至図５のいずれの場合においても不正視聴を阻止可能にしたものである。なお、図２においては受信機側の構成のみを示したが、放送局側の構成は、図１に示すものと同一であってもよく、また、従来と同一であってもよい。即ち、本実施の形態においては、ＥＭＭ中に視聴契約の開始時の情報を含めなくても不正視聴を阻止することができる。

【００７５】図２において、有料放送受信機４５は、ＩＣカード１９に代えてＩＣカード４０を採用した点が図１の有料放送受信機１０と異なる。ＩＣカード４０は、ＥＭＭ暗号化／復号化部２８に代えてＥＭＭとＥＣＭ暗号化／復号化部４１を採用し、視聴可否判定部２６に代えて視聴可否判定部４２を採用した点がＩＣカード１９と異なる。

【００７６】ＥＭＭとＥＣＭ暗号化／復号化部４１には、ＥＭＭメモリ２４からＥＭＭが入力されるだけでなく、ＥＣＭ復号化部２１から復号されたＥＣＭも入力されるようになっている。ＥＭＭとＥＣＭ暗号化／復号化部４１は、入力されたＥＣＭ，ＥＭＭを組み合わせて暗号化し、暗号化したＥＣＭ，ＥＭＭを端子３４を介して記録装置３５に出力するようになっている。ＥＣＭ，ＥＭＭが組み合わされて暗号化されていることから、復号化しなければ、ＥＣＭ，ＥＭＭを取り出すことはできない。即ち、ＥＣＭ，ＥＭＭの一方のみを、復号化せずに取り出すことはできない。

【００７７】記録装置３５は、端子３４からのＥＣＭ，ＥＭＭを番組データに対応させて記録媒体に記録する。記録装置３５は、番組データの再生時には、対応するＥＣＭ，ＥＭＭを再生して端子３４からＩＣカード４０に供給するようになっている。

【００７８】ＥＭＭとＥＣＭ暗号化／復号化部４１は、端子３４を介して入力されたＥＣＭ，ＥＭＭを復号化し、セレクタ２５を介して視聴可否判定部４２に出力すると共に、復号化したＥＭＭ中のワーク鍵Ｋｗ をＥＣＭ復号化部２１に供給するようになっている。

【００７９】視聴可否判定部４２は、再生時には、ＥＭＭとＥＣＭ暗号化／復号化部４１からのＥＭＭ及びＥＣＭを視聴可否の判定に用いる。即ち、視聴可否判定部４２は、ＥＭＭとＥＣＭ暗号化／復号化部４１からのＥＣＭとＥＣＭ復号化部２１からのＥＣＭとの一致を検出し、一致している場合にのみ視聴可否の判定が正当であるものとし、そうでない場合には、視聴不可の判定を行うようになっている。

【００８０】上述したように、ＥＣＭ内には、ＥＭＭの契約の期限と比較判定するための日時情報（年月日時分秒等）が含まれている。視聴可否判定部４２は、例えば、日時情報内の所定部分が一致することによって同一性を判定する。例えば、日時情報中の年月の情報を用いる。この場合には、１ヶ月内の不正視聴を阻止することができるが、契約の単位が１月単位であれば十分である。更に、例えば、年月日又は年月日時まで判定することによって、一層厳密な同一性判定が可能となる。例えば、視聴契約が日毎で変更可能な場合には、年月日を同一性判定の基準にすると、その日内の番組に対して不正視聴の危険性がある。システムを適用する放送局の意向に従って、同一性判定のための判定基準を設定すればよい。

【００８１】次に、このように構成された実施の形態の動作について説明する。

【００８２】録画時には、選局回路１２からスクランブルされたままの番組データを記録装置３２に供給する。また、ＥＭＭとＥＣＭ暗号化／復号化部４１には、ＥＭＭメモリ２４及びＥＣＭ復号化部２１から、記録する番組に対応したＥＭＭとＥＣＭとが入力される。ＥＭＭとＥＣＭ暗号化／復号化部４１は、入力されたＥＣＭ，ＥＭＭを組にして、組となったＥＣＭ，ＥＭＭを暗号化する。ＥＭＭとＥＣＭ暗号化／復号化部４１の出力は、端子３４を介して記録装置３５に供給され、番組と共に記録される。

【００８３】再生時には、記録装置３５は、スクランブルされた番組データを端子３３を介して切り替え回路１３に出力すると共に、暗号化されたＥＣＭ，ＥＭＭの組を端子３４を介してＩＣカード４０のＥＭＭとＥＣＭ暗号化／復号化部４１に出力する。

【００８４】ＥＭＭとＥＣＭ暗号化／復号化部４１は暗号化されているＥＣＭ，ＥＭＭを復号し、ＥＣＭ，ＥＭＭの組をセレクタ２５を介して視聴可否判定部４２に出力する。また、ＥＭＭとＥＣＭ暗号化／復号化部４１は、ＥＣＭＭをＥＣＭ復号化部２１にも出力する。ＥＣＭ復号化部２１は、分離回路１４から再生番組中のＥＣＭが与えられ、ＥＭＭ中のワーク鍵Ｋｗ を用いて復号化し、復号したＥＣＭを視聴可否判定部４２に出力する。

【００８５】視聴可否判定部４２は、再生する番組についての視聴可否を判定する場合には、ＥＭＭと組になって入力されたＥＣＭがＥＣＭ復号化部２１からのＥＣＭに一致するか否かを判定する。視聴可否判定部４２は、入力された２つのＥＣＭを一致と判定した場合にのみ、

視聴可否判定を有効とし、そうでない場合には、視聴不可と判定する。

【００８６】ここで、ユーザの不正によって、記録装置３５から再生された番組と対応しないＥＭＭ，ＥＣＭの組がＩＣカード４０に入力されるものとする。この場合でも、例えば、番組Ｂ，Ｃ等に対する視聴契約が図５に示す状況であるものとし、視聴契約が結ばれていない番組Ｃの再生時に、視聴契約された番組Ｂに対応するＥＭＭとＥＣＭの組がＩＣカード４０に入力されるものとする。なお、番組Ｂに対応するＥＭＭは、従来と同様の視聴可否の判定方法によれば、番組Ｃの復号を可能にするものとする。

【００８７】この場合においても、ＥＣＭ復号化部２１は、ＥＭＭとＥＣＭ暗号化／復号化部４１からのＥＭＭを用いて、ＥＣＭを復号化可能である。しかし、視聴可否判定部４２は、ＥＣＭ復号化部２１からのＥＣＭとＥＭＭとＥＣＭ暗号化／復号化部４１からのＥＣＭとの一致を判定する。ＥＣＭは番組を特定する情報を有しているので、視聴可否判定部４２は、ＥＭＭとＥＣＭ暗号化／復号化部４１からのＥＣＭとＥＣＭ復号化部２１からのＥＣＭが不一致であることを判定することができる。

【００８８】視聴可否判定部４２は、入力された２つのＥＣＭが不一致であると判定したことにより、ＩＣカード４０に入力された再生番組の視聴は不可であるものと判定する。即ち、この場合には、デスクランブラ１５にはデスクランブル鍵は供給されない。

【００８９】なお、本実施の形態によれば、ＥＭＭに視聴契約開始時の情報を含めることなく、図３及び図４の例においても、不正視聴を防止することができることは明らかである。

【００９０】このように、本実施の形態においては、ＥＭＭとＥＣＭとを組にして暗号化し、再生番組の復号にＥＭＭを用いる場合には、このＥＭＭと組になったＥＣＭもＩＣカード４０に取込むようになっており、入力される番組データから得たＥＣＭと記録装置３５から得たＥＣＭとの一致判定を行うことで、不正視聴を確実に防止することができる。

【００９１】なお、視聴可否判定部４２の同一性判定の手法としては種々の手法が考えられる。例えば、ＥＣＭ内に番組番号を配置し、これを利用してもよい。番組番号を、いわゆる番組毎に割り当てることにより、ＥＣＭの一致比較から他の番組用のＥＭＭを復号に利用することができなくなる。

【００９２】また、同一性判定のその他の方法として、ＥＣＭ内に含まれるデスクランブル鍵以外の情報が一致するか否かを判定するようにしてもよい。更に、ＥＣＭの判定の細かさを、ＥＣＭで指定してもよい。すなわち、番組再生時に、ＥＣＭで指定された細かさにより、同一性判定の方法を変えるのである。ＩＣカード４０内に入力される番組データのＥＣＭに、同一性判定の方法として日時情報を使用し、細かさが年月までとなっている場合には、同一性判定の方法として番組番号を使用する場合など指定する。このようにすることによって、放送局の意向を番組毎に反映させた判定が可能となる。

【００９３】

【発明の効果】以上説明したように本発明によれば、タイムシフト視聴を可能にした場合でも、不正視聴を確実に防止することができるという効果を有する。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る有料放送システム及び有料放送受信機を示すブロック図。

【図２】本発明の他の実施の形態を示すブロック図。

【図３】従来例における問題点を説明するための説明図。

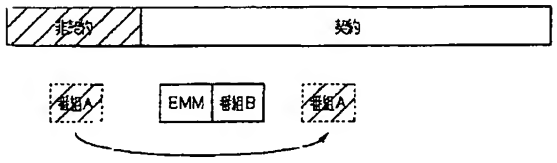
【図４】従来例における問題点を説明するための説明図。

【図５】従来例における問題点を説明するための説明図。

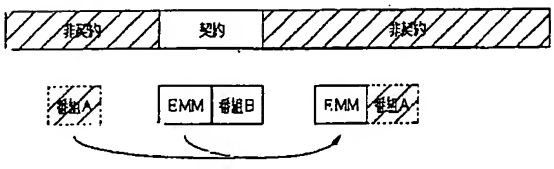
【符号の説明】

１…放送局、６…ＥＭＭ生成／暗号化部、１０…有料放送受信機、１５…デスクランブラ、１９…ＩＣカード、２１…ＥＣＭ復号化部、２２…ＥＭＭ復号化部、２６…視聴可否判定部、２８…ＥＭＭ暗号化／復号化部、３５…記録装置。

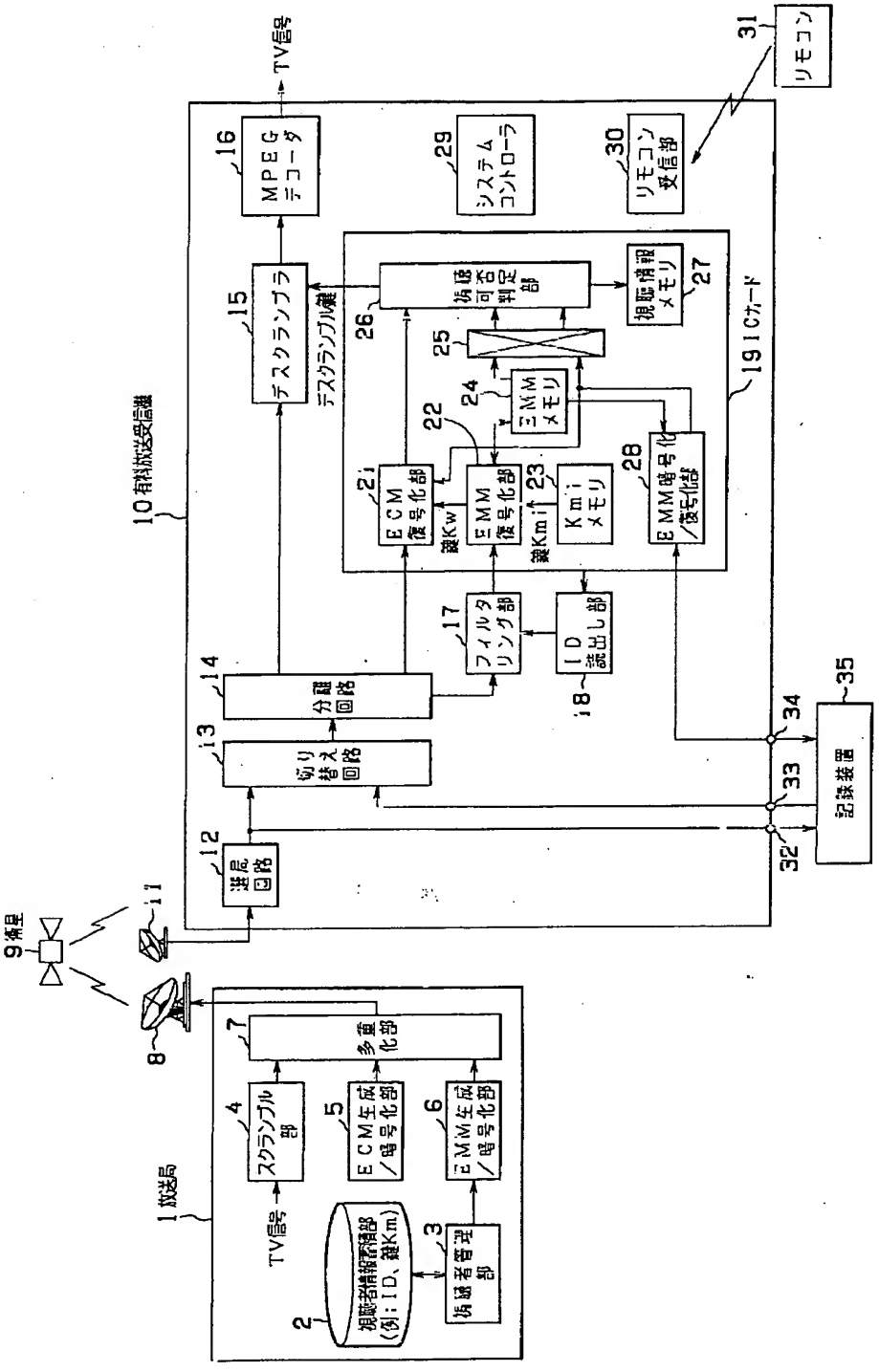
【図３】



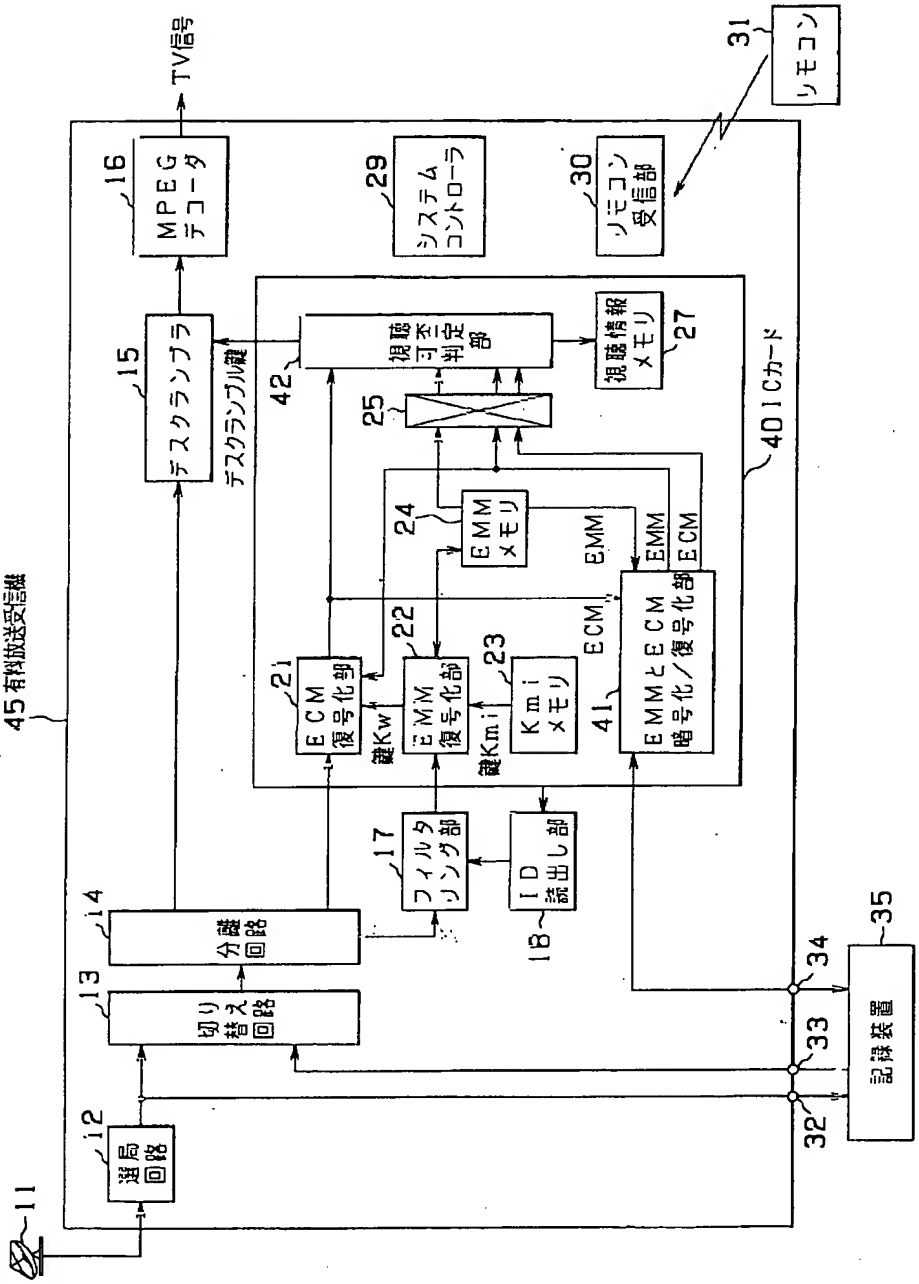
【図４】



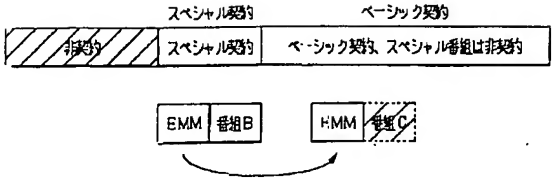
【図1】


1 放送局
2 視聴者情報蓄積部 (例:ID、鍵Km)
3 視聴者管理部
4 スクランブル部
5 ECM生成/暗号化部
6 EMM生成/暗号化部
7 多重化部
8
9 衛星
10 有料放送受信機
11
12 混信回路
13 切り替え回路
14 分離回路
15 デスクランブラ
16 MPEGデコーダ
17 フィルタリング部
18 ID読出し部
19 ICカード
21 ECM復号化部
22
23 Kmiメモリ
24 EMMメモリ
25
26 視聴可否判定部
27 視聴情報メモリ
28 EMM暗号化/復号化部
29 システムコントローラ
30 リモコン受信部
31 リモコン
32
33
34
35 記録装置
TV信号
TV信号
デスクランブル鍵
鍵Kw
鍵Kmi

【図2】


TV信号
MPEG デコーダ
16
システム コントローラ
29
リモコン 受信部
30
リモコン
31
デスクランブラ
15
デスクランブル鍵
42
視聴 可否 判定 部
視聴情報 メモリ
27
25
ICカード
40
EMM メモリ
24
EMM
ECM
ECM 復号化部
21
EMM 復号化部
22
Kmi メモリ
23
EMMとECM 暗号化/復号化部
41
鍵Kw
鍵Kmi
フィルタ リング部
17
ID 読出し部
18
分離 回路
14
切り 替え 回路
13
選局 回路
12
11
有料放送受信機
45
記録装置
35
34
33
32

【図5】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI			(参考)
H04N	5/44		H04N	7/167	Z	5J104
	5/76		H04L	9/00	601B	
	5/91				621A	
	7/08		H04N	5/91	P	
	7/081			7/08	Z	
// H04N	7/20	630				

Fターム(参考) 5C025 AA23 AA30 BA25 BA27 BA30
DA01 DA04 DA05
5C052 AA01 DD04
5C053 FA20 FA21 FA23 HA40 JA30
LA07
5C063 AB03 AB07 AC10 CA40
5C064 CA18 CB01 CC01 DA01
5J104 AA01 AA16 BA03 EA01 EA07
EA17 NA03 NA35 NA37 PA04
PA05